CORRECTED Amendments to the Claims

This listing of the claims is responsive to the Notice of Non-Compliant Amendment in the Official Action and replaces the Amendments to the Claims in the response filed September 22, 2008.

Listing of Claims

1. (currently amended) A security system for repelling malicious software ~~softwares in computers and computer networks and that is configured to forward messages~~, the security system comprising a first sub-system to detect an unknown malicious software ~~softwares~~ having a characteristic ~~one or more characteristics~~ unknown to said first sub-system, said first sub-system being configured, in connection with the forwarding of messages or with other action or, in a timed manner, to perform ~~at least~~ a partial simulation to activate the unknown malicious software ~~softwares~~ having the characteristic ~~one or more characteristics~~ unknown to said first sub-system for causing a consequence of an activation of the unknown malicious software and thereafter to detect the activated unknown malicious software ~~softwares~~ by detecting the consequence of the ~~consequences of~~ activation of the unknown malicious software ~~softwares~~.

2. (currently amended) The security system in accordance with Claim 1, ~~that is adapted~~ configured to forward an alarm

caused by the detection of the malicious software ~~softwares~~ to at least one system connected to the security system.

3. (currently amended) The security system in accordance with Claim 1, ~~that is further adapted~~ configured to break a connection to at least one other system on the basis of an alarm caused by the detection of the malicious software ~~softwares~~.

4. (previously presented) The security system in accordance with Claim 1, further comprising a second sub-system for forwarding messages from the first sub-system to at least one system connected to the security system.

5. (currently amended) The security system in accordance with Claim 1, further comprising a third sub-system configured ~~that is adapted~~ to break a connection to at least one other sub-system upon receiving an alarm.

6. (previously presented) The security system in accordance with Claim 5, wherein the at least one other sub-system includes an identifier which corresponds to an identifier of the third sub-system.

7. (canceled)

8. (previously presented) The security system in accordance with Claim 2, wherein the alarm is a message or at least a part of a message that is forwarded to the recipient prior to other communications.

9. (previously presented) The security system in accordance with Claim 5, wherein the third sub-system includes at least one computer or one network element including a computer.

10. (previously presented) The security system in accordance with Claim 2, wherein the alarm is forwarded via a separate connection.

11. (canceled)

12. (currently amended) The security system in accordance with Claim 1, wherein the consequence ~~consequences~~ of activation of the malicious software ~~softwares~~ detected by the first sub-system ~~include~~ includes at least one of: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect the malicious software ~~softwares~~, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there.

13. (canceled)

14. (currently amended) The security system in accordance with Claim 1, wherein the first sub-system chooses ~~is adapted to choose~~ one or more of the following logics when trying to

activate the malicious software ~~softwares~~: one defined by the user, pre-programmed or at least partially random logic.

15. (currently amended) The security system in accordance with Claim 5, further comprising a parallel system that saves ~~is adapted to save~~ a message sent from the third sub-system, the parallel system being connected in parallel with the third sub-system.

16. (currently amended) The security system in accordance with Claim 15, wherein the first sub-system compares ~~is adapted to compare~~ in the parallel system a message sent from the third sub-system to the first sub-system and additionally saved in the parallel system in order to detect an anomaly caused by a malicious software.

17. (currently amended) The security system in accordance with Claim 15, wherein the parallel system forwards ~~is adapted to forward~~ a message saved by it.

18. (currently amended) The security system in accordance with Claim 1, that examines ~~is adapted to examine~~ messages forwarded through the security system in order to detect known malicious software ~~softwares~~.

19. (currently amended) The security system in accordance with Claim 4, comprising first and second ones of the at least one system, wherein the security system transfers ~~is adapted to transfer~~ data between the first and the second ones of the at least one system through the first and the second sub-systems,

and wherein the security system disrupts ~~is adapted to disrupt~~ the connection between the first one of the at least one system and the first sub-system before a connection is established between the first and the second sub-systems and disrupts ~~to disrupt~~ the connection between the first and the second sub-systems before a connection is established between the second sub-system and the second one of the at least one system.

20. (currently amended) The security system in accordance with claim 1, wherein said first sub-system compares ~~is adapted to compare~~ messages with at least partially identical identifiers with each other in order to detect the unknown malicious software ~~softwares~~.

21. (currently amended) The security system in accordance with Claim 20, wherein the first sub-system requests ~~is adapted to request~~ the sender of the messages with at least partially identical identifiers to re-send at least one of the messages and [[is]] further compares ~~adapted to compare~~ at least one re-sent message received with the original messages in order to detect messages containing the malicious software ~~softwares~~.

22. (currently amended) A method for repelling malicious software ~~softwares in computers and data networks~~, the method being carried out in a security system including a first sub-system for forwarding messages and for detecting an unknown malicious software ~~softwares~~ having a characteristic ~~one or more characteristics~~ unknown to said first sub-system and that is

isolatable from a remainder of the security system, the method includes the steps ~~where~~:

- in a partial simulation, activating the unknown malicious software having the characteristic unknown to said first sub-system to cause a consequence of the activation,

- monitoring functions of the security system ~~are monitored~~ by the first sub-system in order to detect the consequence ~~consequences~~ of the activation, in the ~~an at least~~ partial simulation, of [[an]] the unknown malicious software ~~having one or more characteristics unknown to said first sub-system, when consequences~~, the consequence of activation including at least one of the following: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a malicious software, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there,

- thereafter detecting the unknown [[a]] malicious software ~~is detected~~ when one of the consequences is detected, and

- giving an alarm ~~is given~~.

23. (currently amended) A method for repelling malicious software ~~softwares in computers and computer networks~~, the method comprising the steps of:

performing ~~an at least~~ a partial simulation to activate an unknown malicious software ~~softwares~~ having a characteristic ~~one or more characteristics~~ unknown to an entity performing the method in connection with the forwarding of messages or other action, or in a timed manner, the activation for causing a consequence of the activation,

thereafter detecting the activated unknown malicious software ~~softwares~~ by detecting the consequence ~~consequences~~ of the activation of the unknown malicious software ~~softwares~~ caused by the ~~at least~~ partial simulation, and

giving an alarm when a malicious software is detected.

24-25. (canceled)

26. (currently amended) The method in accordance with Claim 23, wherein the method is run in a security system including a first sub-system and a second sub-system and wherein the consequence ~~consequences~~ of activation of the malicious software ~~include~~ includes at least one of: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a malicious software, a message leaves for another system without command from the first sub-system, a message leaves for

another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there.

27-28. (canceled)

29. (currently amended) The method in accordance with Claim 23, further comprising the step where the known malicious software is ~~softwares are~~ searched for on the basis of its ~~their~~ characteristics.

30. (previously presented) The method in accordance with Claim 26, wherein the security system is connected to a first system and a second system and wherein data are transferred between the first system and the second system through the first sub-system and the second sub-system phase by phase in order, in which phases:

- the connection for data transfer is disrupted between the first system and the first sub-system,

- a connection for data transfer is established between the first sub-system and the second sub-system,

- the connection for data transfer is disrupted between the first sub-system and the second sub-system,

- a connection for data transfer is established between the second sub-system and the second system.

31. (currently amended) An apparatus for repelling malicious software ~~softwares in computers and computer networks~~, comprising equipment for saving data and for handling data and

equipment for transferring data with another apparatus, wherein the apparatus is configured to receive a message and to perform ~~an at least~~ a partial simulation to activate the unknown malicious software ~~softwares~~ having a characteristic ~~one more characteristics~~ unknown to the apparatus and contained in the message, the activation for causing a consequence of the activation, and thereafter to detect the activated unknown malicious softwares by detecting the consequence ~~consequences~~ of the activation of the unknown malicious software ~~softwares~~.

32. (canceled)

33. (currently amended) The apparatus in accordance with Claim 31, wherein the consequence ~~consequences~~ of activation of the malicious software includes ~~include~~ at least one of: a change takes place prior to actions caused by changes made by the apparatus, a change takes place that is not an action taken by the apparatus to detect a malicious software.

34. (currently amended) The apparatus in accordance with Claim 31, wherein the apparatus sends ~~is adapted to send~~ a message to either a sub-assembly of the apparatus or to said another apparatus, and wherein the consequence ~~consequences~~ of activation of the malicious software includes ~~include~~ at least one of: a message leaves without authorization from the anti-malicious software of the apparatus, a message leaves for an address it has not originally been directed to, a message does not leave although it has been given a command to be sent.

35-36. (canceled)

37. (currently amended) The apparatus in accordance with Claim 31, wherein the apparatus examines the message in order to detect known malicious software ~~softwares~~.

38-39. (canceled)

40. (previously presented) The security system in accordance with Claim 1, wherein the security system communicates with the computer network being protected by the security system, but is separate from the computer network.

41. (previously presented) The security system in accordance with Claim 40, wherein the security system is in a gateway for the computer network.

Amendments to the Claims

This listing of the claims is responsive to the present Official Action and replaces all prior versions and listing of the claims in the present application, including the CORRECTED Amendments to the Claims above.

Listing of Claims

1. (currently amended) A security system ~~for repelling malicious software, the security system~~ comprising:

a first sub-system configured to detect in said first sub-system an unknown malicious software having a characteristic unknown to said first sub-system, and

said first sub-system being configured~~, in connection with the forwarding of messages or with other action or, in a timed manner,~~ to perform a partial simulation in said first sub-system for activating ~~to activate~~ the unknown malicious software having the characteristic unknown to said first sub-system for causing a consequence of an activation of the unknown malicious software in said first sub-system and thereafter to detect the activated unknown malicious software in said first sub-system by detecting the consequence of the activation of the unknown malicious software in said first sub-system.

2. (previously presented) The security system in accordance with Claim 1, configured to forward an alarm caused by the

detection of the malicious software to at least one system connected to the security system.

3. (previously presented) The security system in accordance with Claim 1, configured to break a connection to at least one other system on the basis of an alarm caused by the detection of the malicious software.

4. (previously presented) The security system in accordance with Claim 1, further comprising a second sub-system for forwarding messages from the first sub-system to at least one system connected to the security system.

5. (previously presented) The security system in accordance with Claim 1, further comprising a third sub-system configured to break a connection to at least one other sub-system upon receiving an alarm.

6. (previously presented) The security system in accordance with Claim 5, wherein the at least one other sub-system includes an identifier which corresponds to an identifier of the third sub-system.

7. (canceled)

8. (previously presented) The security system in accordance with Claim 2, wherein the alarm is a message or at least a part of a message that is forwarded to the recipient prior to other communications.

9. (previously presented) The security system in accordance with Claim 5, wherein the third sub-system includes at least one computer or one network element including a computer.

10. (previously presented) The security system in accordance with Claim 2, wherein the alarm is forwarded via a separate connection.

11. (canceled)

12. (previously presented) The security system in accordance with Claim 1, wherein the consequence of activation of the malicious software detected by the first sub-system includes at least one of: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect the malicious software, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there.

13. (canceled)

14. (previously presented) The security system in accordance with Claim 1, wherein the first sub-system chooses one or more of the following logics when trying to activate the malicious software: one defined by the user, pre-programmed or at least partially random logic.

15. (previously presented) The security system in accordance with Claim 5, further comprising a parallel system that saves a message sent from the third sub-system, the parallel system being connected in parallel with the third sub-system.

16. (previously presented) The security system in accordance with Claim 15, wherein the first sub-system compares in the parallel system a message sent from the third sub-system to the first sub-system and additionally saved in the parallel system in order to detect an anomaly caused by a malicious software.

17. (previously presented) The security system in accordance with Claim 15, wherein the parallel system forwards a message saved by it.

18. (previously presented) The security system in accordance with Claim 1, that examines messages forwarded through the security system in order to detect known malicious software.

19. (previously presented) The security system in accordance with Claim 4, comprising first and second ones of the at least one system, wherein the security system transfers data between the first and the second ones of the at least one system through the first and the second sub-systems, and wherein the security system disrupts the connection between the first one of the at least one system and the first sub-system before a connection is established between the first and the second sub-systems and disrupts the connection between the first and the second sub-

systems before a connection is established between the second sub-system and the second one of the at least one system.

20. (previously presented) The security system in accordance with claim 1, wherein said first sub-system compares messages with at least partially identical identifiers with each other in order to detect the unknown malicious software.

21. (previously presented) The security system in accordance with Claim 20, wherein the first sub-system requests the sender of the messages with at least partially identical identifiers to re-send at least one of the messages and further compares at least one re-sent message received with the original messages in order to detect messages containing the malicious software.

22. (currently amended) A method for repelling malicious software, the method being carried out in a security system including a first sub-system for forwarding messages and that is configured to detect ~~for detecting~~ an unknown malicious software having a characteristic unknown to said first sub-system and that is isolatable from a remainder of the security system, the method includes the steps:

- detecting in said first sub-system the unknown malicious software having a characteristic unknown to said first sub-system,

- ~~in a~~ performing a partial simulation in said first sub-system for[[,]] activating the unknown malicious software having

the characteristic unknown to said first sub-system to cause a consequence of the activation in said first sub-system,

- monitoring functions of the security system by the first sub-system in order to detect the consequence of the activation in said first sub-system, in the partial simulation, of the unknown malicious software, the consequence of activation including at least one of the following: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a malicious software, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there,

- thereafter detecting in said first sub-system the unknown malicious software by detecting [[when]] one of the consequences ~~is detected~~ in said first sub-system, and

- giving an alarm.

23. (currently amended) A method for repelling malicious software, the method comprising the steps of:

detecting in a first sub-system of a security system an unknown malicious software having a characteristic unknown to said first sub-system;

performing a partial simulation in the first sub-system to activate [[an]] the detected unknown malicious software having a characteristic unknown to said first sub-system ~~an entity performing the method in connection with the forwarding of messages or other action, or in a timed manner~~, the activation for causing a consequence of the activation in said first sub-system,

thereafter detecting the activated unknown malicious software in said first sub-system by detecting the consequence of the activation in said first sub-system of the unknown malicious software caused by the partial simulation, and

giving an alarm when a malicious software is detected.

24-25. (canceled)

26. (currently amended) The method in accordance with Claim 23, ~~wherein the method is run in a security system including a first sub-system and a second sub-system and~~ wherein the consequence of activation of the malicious software includes at least one of: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a malicious software, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed

to, and a message does not leave for another system although it has been sent there.

27-28. (canceled)

29. (currently amended) The method in accordance with Claim 23, further comprising the step of searching for ~~where the~~ known malicious software ~~is searched for~~ on the basis of its characteristics.

30. (currently amended) The method in accordance with Claim 26, wherein the security system is connected to a first system and a second system and wherein data are transferred between the first system and the second system through the first sub-system and [[the]] a second sub-system phase by phase in order, in which phases:

- the connection for data transfer is disrupted between the first system and the first sub-system,

- a connection for data transfer is established between the first sub-system and the second sub-system,

- the connection for data transfer is disrupted between the first sub-system and the second sub-system,

- a connection for data transfer is established between the second sub-system and the second system.

31. (currently amended) An apparatus for repelling malicious software, comprising equipment for saving data and for handling data and equipment for transferring data with another apparatus, wherein the apparatus is configured to receive a

message and to detect in the apparatus an unknown malicious software contained in the message and having a characteristic unknown to the apparatus, the apparatus being configured to perform a partial simulation in the apparatus to activate the unknown malicious software having a characteristic unknown to the apparatus and contained in the message, the activation [[for]] causing a consequence of the activation in the apparatus, and thereafter the apparatus detecting ~~to detect~~ the activated unknown malicious software ~~softwares~~ by detecting the consequence of the activation of the unknown malicious software in the apparatus.

32. (canceled)

33. (previously presented) The apparatus in accordance with Claim 31, wherein the consequence of activation of the malicious software includes at least one of: a change takes place prior to actions caused by changes made by the apparatus, a change takes place that is not an action taken by the apparatus to detect a malicious software.

34. (previously presented) The apparatus in accordance with Claim 31, wherein the apparatus sends a message to either a sub-assembly of the apparatus or to said another apparatus, and wherein the consequence of activation of the malicious software includes at least one of: a message leaves without authorization from the anti-malicious software of the apparatus, a message leaves for an address it has not originally been directed to, a

message does not leave although it has been given a command to be sent.

35-36. (canceled)

37. (previously presented) The apparatus in accordance with Claim 31, wherein the apparatus examines the message in order to detect known malicious software.

38-39. (canceled)

40. (previously presented) The security system in accordance with Claim 1, wherein the security system communicates with the computer network being protected by the security system, but is separate from the computer network.

41. (previously presented) The security system in accordance with Claim 40, wherein the security system is in a gateway for the computer network.